Remarks

In the Office Action dated April 8, 2005, the Examiner rejected claims 1-4, 8-11, 13-16 and 20-23 under 35 U.S.C. § 103 as being unpatentable over the U.S. Patent to Bahlmann 6,487,594 in view of the U.S. Patent to Brownlie, et al. 6,202,157. The Examiner rejected claims 5-7, 12, 17-19 and 24 under 35 U.S.C. § 103 as being unpatentable over Bahlmann in view of Brownlie, et al. and further in view of the U.S. Patent to Moriconi, et al. 6,158,010.

Initially, the present invention relates to a method and system for determining and enforcing security policy in a communication session (i.e., title and object of the invention). Local and group policies are provided wherein each local policy states a set of local requirements for the session for a participant and the group policy represents a set of conditional, security-relevant requirements to support the session. The policy instance is generated based on the group and local policies. A policy instance defines a configuration of security-related services used to implement the session and rules used for authorization and access control of participants to the session. The policy instance is analyzed with respect to a set of correctness principles. The policy instance is distributed to the participants and the security policy is enforced based on the rules throughout the session.

Clearly, none of the references of record taken either alone or in combination with one another disclose the invention as claimed in each of the independent claims.

For example, the U.S. Patent to Bahlmann provides a policy management system for an Internet service provider having Internet provisioning servers in different regions. The system includes regional policy databases (RPDs) and a central policy database (CPD). Each RPD stores Internet provisioning data and each is associated with the Internet provisioning servers in a respective region. The Internet provisioning servers use the Internet provisioning data of their associated RPD to provision Internet service in the respective region. The CPD stores product objects, feature objects, and other objects such as device objects and subscriber objects. The objects of the CPD are operable with the stored data of the RPDs for

providing central definitions of quality of service provisioning policies and level of service provisioning policies to the Internet provisioning servers.

The policy management system of Bahlmann provides centralized configuration and local management of the policies which control aspects of service and level qualities of the Internet provisioning servers. The policy management system links various aspects of the Internet provisioning servers to the CPD. The CPD distributes central product definitions to the Internet provisioning servers via the RPDs.

As noted in the Background Art section of the application, the U.S. Patent to Brownlie, et al. describes how policy data can contain provisioning information. The example provisioning data identified include password lengths, password aging, cryptographic algorithms, and key lengths. The policy data is centrally defined and digitally signed. It is then distributed to all the network nodes, who verify the digital signature, and then install the policy. However, there is no notion of access control policies and no general purpose enforcement architecture is described, and there is no notion of events.

As also noted in the Background Art section of the application, the U.S. Patent to Moriconi, et al. describes a method for security policy distribution from a central node to clients where the security policy specifies access control to securable components. With respect to distribution, the security policy corresponds to a policy instance. However, there is also no support for provisioning of mechanisms in the policies. It only supports access control. Access control rules can have conditions. However, there is no support for reconfiguration of a policy when an operation is attempted. The access control language is general (it allows DENY statements); thus it would be difficult to support automated policy analysis reconciliation, or compliance checking with other policies. Policy analysis to determine if a policy satisfies a given set of assertions is not provided. The policy analysis is used to query policy rules rather than determine satisfaction of a set of assertions. There is no support for reconciling group and local policies to determine a policy instance or checking compliance of a local policy with a policy instance, etc.

In view of the above, it is clear that none of the references utilized by the Examiner in rejecting the claims, teach, disclose or discuss either alone or in combination with one another, the generation of a policy instance based on group and local policies wherein the policy instance defines a configuration of security-related services used to implement the session and rules used for authorization and access control of participants to the session. The group policy of the present invention represents a set of conditional, security-relevant requirements to support the session. Bahlmann fails to show such a group policy. Bahlmann distributes central product definitions. The policies of Bahlmann control aspects of service and level qualities. Bahlmann fails to distribute a policy instance which defines a configuration of security-related services used to implement the session.

Consequently, in view of the above and in the absence of better art Applicants' Attorney respectfully submits the application is in condition for allowance which allowance is respectfully requested.

Respectfully submitted,

Patrick D. McDaniel, et al.

By_____

David R. Syrowik
Reg. No. 27,956
Attorney/Agent for Applicant

Date: June 10, 2005

BROOKS KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075-1238
Phone: 248-358-4400
Fax: 248-358-3351